Defense Security Service

National Industrial Security Program

NISP

AN OVERVIEW OF
THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

Background

U.S. industry develops and produces the majority of our nation's defense technology-much of which is classified-and thus plays a significant role in creating and protecting the information that is so vital to our national security. The National Industrial Security Program (NISP) was established to ensure that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.

Authority

The NISP was established by Executive Order 12829, January 6, 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12958, April 17, 1995, "Classified National Security Information," and the Atomic Energy Act of 1954, as amended.

Responsibilities

The National Security Council is responsible for providing overall policy direction for the NISP. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP, and for issuing directives that agencies under the NISP are required to implement.

The Secretary of Defense (SECDEF) serves as the Executive Agent for the NISP. There are, however, four Cognizant Security Agencies (CSAs) under the NISP, including the Department of Defense, Department of Energy, Central Intelligence Agency, and the Nuclear Regulatory Commission. The SECDEF with the concurrence of the Secretary of Energy, Chairman of the Nuclear Regulatory Commission, and Director of Central Intelligence is responsible for the issuance and maintenance of the DoD 5220.22M, "National Industrial Security Program Operating Manual" (NISPOM). (Note: The NISPOM may be downloaded from the DSS Web Site at www.dss.mil.)

Implementation

The Defense Security Service (DSS) administers the NISP on behalf of the DoD and 22 non-DoD federal agencies within the Executive Branch of the federal government. The DSS Industrial Security Representative (ISR) is the principal interface with cleared industry under the defense portion of the NISP. DSS has approximately 240 ISRs who provide oversight, advice, and assistance to over 11,000 contractor facilities that are cleared for access to classified information. The ISR works in a professional partnership with the contractor's facility management staff and Facility Security Officer (FSO) in formulating threat appropriate and cost effective security programs to ensure the protection of classified information released under contractual obligations or research and development efforts. In addition, the ISR interacts with the government customers on facility clearance issues that may have an affect on the ability of the contractor to perform on the classified contract. The DSS Counterintelligence (CI) office assists the ISRs in the integration of CI into their oversight, and advice, and assistance roles with cleared defense industry. DSS also has a small cadre of information system security personnel who assist ISRs and contractor personnel in accrediting automated information systems to process classified information.

Frequenty Asked Questions About the NISP

What is a Facility?

Under the NISP the term "facility" refers to a designated operating entity in private industry or at a college/university, such as a plant, lab, office, or commercial structure with associated warehouse space, storage areas, utilities, and components which are related by function or location. Federal government installations, or portions of, are not considered facilities under the NISP.

Does DSS Have Security Cognizance Over a Contractor Facility Located on a Military Installation Within the U.S., Puerto Rico, U.S. Possession or Trust Territory?

At the request of the responsible U.S. Military Commander for the installation, DSS may exercise security cognizance over a contractor facility on

the installation if the organization is within the U.S., Puerto Rico, U.S., possession or trust territory. If DSS officially accepts the commander's request, a DSS ISR will then be assigned to provide security oversight to the facility in accordance with the requirements of the NISPOM.

What is a Facility Security Clearance (FCL)?

From a national security standpoint, a Facility Security Clearance (FCL) is an administrative determination that a facility is eligible to access classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or Top Secret level. In order to obtain an FCL, the contractor must execute a Department of Defense Security Agreement (DD Form 441) or Appendage to Department of Defense Security Agreement (DD Form 441-1). The DD Form 441 is a legally binding document that sets forth the responsibilities of both parties, and obligates the contractor to abide by the security requirements of the NISPOM. The DD Form 441-1 extends the terms and conditions of the agreement to branch offices of the contractor.

Who Can Request an FCL?

A contractor or prospective contractor cannot apply for its own FCL. A Government customer or a currently cleared facility must sponsor an uncleared contractor for an FCL based on a bona fide procurement requirement to access classified information.

What Format and Information Are Required in an FCL Request?

There is no required format; however, the request must be signed and provided on the letterhead of the requesting government activity or prime contractor. To accept and process the request for an FCL, DSS needs the:

- Facility's name and address.

- Name, title, phone number, and (if available) email address of the facility's point of contact.

- Identification of the bona fide procurement requirement to gain access to classified information (if at all possible, the contract, program, or bid number), level of the clearance needed, and whether classified safe-

guarding (and at what level) will be required on the premises of the contractor's facility.

- Completed “Department of Defense Contract Security Classification Specification" (DD Form 254)—if it is available.

- Identification of special requirements associated with the request, such as special briefings, an Interim Top Secret FCL, or personnel clearances.

- The requestor's organization or company name, address, the point of contact's name, title, phone number and (if available) email address.

Who Accepts the New FCL Requests?

FCL request should be mailed or faxed to:

The Defense Industrial Security Clearance Office (DISCO)
ATTN: Facility Clearance Division
2780 Airport Drive, Suite 400
Columbus, OH 43219-2268.
FAX: 614-827-1586

Are There Any Other Eligibility Requirements for an FCL Besides a Legitimate U.S. Government or Foreign Government Requirement for Access to Classified Information?

Yes. The contractor must be organized and exist under the laws of one or more of the fifty states in the U.S., the District of Columbia, or Puerto Rico, and be located in the U.S. or its territorial areas or possessions. The contractor must have a reputation of integrity and lawful conduct in its business dealings, and the contractor and its key managers must not be barred from participating in U.S. government contracts. In addition, the contractor must not be under foreign ownership, control, or influence (FOCI) to such a degree that the granting of the FCL would be inconsistent with the national interests of the U.S.

How Many Affirmative Responses on the "Certificate Pertaining to Foreign Interests" (SF 328) Determine When the Facility is Under FOCI?

The number of affirmative responses is not the factor that will determine whether a facility is under FOCI. The factors that are considered in the aggregate are the:

- Foreign intelligence threat.

- Risk of unauthorized technology transfer.

- Type and sensitivity of the information requiring protection.

- Nature and extent of the FOCI, to include the source of the FOCI to the ultimate ownership and whether a non-U.S. citizen occupies a controlling or dominant minority position.

- Record of compliance with pertinent U.S. laws, regulations and contracts.

- Nature of the bilateral and multilateral security and information exchange agreements that may be pertinent.

Is There any Coordination with the Government Customer When DSS Analyzes the FOCI Factors and How They Might Be Mitigated?

Yes, DSS coordinates with the federal government customer to ensure that all FOCI issues that may have an adverse impact on performance of classified contracts are considered in crafting an acceptable mitigation method. The degree of coordination from the ISR or, if needed, DSS Headquarters may vary depending upon the nature and extent of the FOCI factors at the facility.

How Long Does it Take to Get an FCL?

The Final FCL will be granted as soon as all final clearance requirements are satisfied. These clearance requirements include the issuance of final personnel clearances for the Key Management Personnel (KMPs), execution of the DoD Security Agreement between the contractor and DSS, and a favorable foreign ownership, control, or influence (FOCI) determination. If the facility is eligible, DISCO will automatically issue an Interim Secret or Interim Confidential FCL—no special request for an interim FCL is required. However, if an Interim Top Secret (TS) FCL is required, the designated authority within the procuring activity must request that an Interim TS FCL be issued.

What is DSS's Role After a Facility Is Cleared?

Once a facility is cleared DSS has oversight authority to evaluate the security operations of the organization. Industrial Security Specialists will visit each facility to conduct periodic security reviews and provide advice and consultations to determine whether effective security systems and procedures are being implemented to protect the classified information in the facility's possession.

DSS security reviews are scheduled on the following basis:

- Annually—Cleared contractors in possession of classified information

- Every 18 Months—Cleared facilities that access classified information only at government installations or other cleared contractors

Security reviews are conducted in partnership with industrial facilities to identify actual and potential security vulnerabilities, develop alternatives, and monitor the solutions developed to improve the protection of classified information by the facility. DSS is also responsible for certifying, accrediting, and evaluating on a continuous basis the automated information systems (AISs) used by cleared industrial facilities to process classified information.

To learn more about DSS
visit our Web site at
http://www.dss.mil

Additional copies may be obtained from DSS at
brochures@mail.dss.mil

Revised April 2001